

AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A master digital data creation device for supplying second digital data obtained by scrambling first digital data to a digital data reproduction device having a recording medium, comprising:

an encryption block generating a first control word based on ~~a specified~~ an allowable number of reproductions specified by the digital data reproduction device and applying a one-way function to the first control word to produce the allowable number of reproductions to generate a second control word;

a scrambler receiving the second control word for scrambling ~~desired~~ the first digital data using the second control word to produce the second digital data; and

an output block outputting the second digital data and the first control word to ~~an external~~ the digital data reproduction device.

2. (Currently Amended) A digital data reproduction device comprising:

an acceptor accepting recording media on which second digital data and a first control word CW_k are recorded, said first control word being generated based on a specified allowable number of reproductions, said second digital data being generated by scrambling desired first digital data using a second control word CW_0 generated by applying a one-way function to the first control word CW_k k times;

a decryption block receiving the first control word CW_k and applying the one-way function to the first control word CW_k k times to produce the second control ~~work~~ word CW_0 ;

a de-scrambler receiving the second digital data and the second control word CW_0 and de-scrambling the second digital data using the second control word CW_0 to produce the first digital data; and

a reproduction unit reproducing the first digital data generated by said de-scrambler,

wherein, after ~~[[the]]~~ every reproduction by said reproduction unit, said decryption block writes a third control word $CW_{(k-1)}$ back to said recording media, said third control word $CW_{(k-1)}$ being generated by applying the one-way function to the first control word CW_k once, and wherein, if the first control word CW_k received from the recording media equals the second control word CW_0 , the de-scrambling by said de-scrambler and the reproduction by said reproduction unit are inhibited.

3. (Currently Amended) The digital data reproduction device according to claim 2, wherein, when a desired number of reproductions, n , is received from some other reproduction device, said decryption block receives the first control word CW_k from the recording media and, if $k \geq n$, applies the one-way function to the first control word CW_k **(k-n)** times to produce the third control word CW_n and applies the one-way function to the first control word CW_k **n** times to produce the fourth control word $CW_{(k-n)}$; ~~if $k < n$, produces the first control word CW_k as the third control word CW_n and produces the second control word CW_0 as the fourth control word $CW_{(k-n)}$~~ ; and records the fourth control word $CW_{(k-n)}$ on the recording media for updating, further comprising:

an output block outputting the second digital data recorded on the recording media, and
the third control word CW_n obtained from the decryption block, to the other reproduction device.